ABM Industries Incorporated Provides Notice of Data Privacy Incident

NEW YORK, April 26, 2019 – ABM Industries Incorporated (the "company") is providing notice of an incident that may affect the security of some personal information. While the company is currently unaware of any actual or attempted misuse of the impacted information, the company is providing this notice with details about the event as well as the steps taken in response.

What Happened? After noting suspicious activity related to certain employee email accounts, the company immediately launched a detailed and exhaustive investigation which determined the company was the victim of an email phishing incident that resulted in unauthorized access to certain employee email accounts between January 8, 2018 and August 7, 2018. The company's investigation included working with leading cyber security experts to investigate the incident and ensure the security of the company's systems. The contents of the email accounts at issue were reviewed through an in-depth manual and programmatic process to determine what sensitive data may have been accessible. On December 26, 2018, the investigation determined that the emails affected by this incident contained certain personal information related primarily to current and former employees.

What Information Was Involved? While the information present in the impacted emails varies by individual, the investigation determined that the information that may have been affected includes: name, Social Security number, bank account/financial information, credit/debit card information, driver's license number, passport number, birth/marriage certificate, medical information, health insurance information, username and password, and unique electronic identifiers related to certain current and former employees. While this information was contained within the impacted email accounts, the company currently has no evidence that any such information experienced attempted or actual misuse.

What the Company is Doing. The company has an ongoing commitment to data security, with a focus on continued improvement, including implementing enhanced security technology, engaging outside security vendors, and enhancing company-wide phishing awareness and cyber-security training. The company provided notification by way of first-class mail to impacted individuals for whom it had available address information. The company is also offering impacted individuals free identity protection and credit monitoring services through Kroll. Additionally, the company is providing written guidance on how consumers can better protect themselves against identity theft and fraud, which includes reporting any suspicious account activity to their credit card company and/or bank, as well as encouraging individuals whose username and password information was impacted to change their login credentials. As part of its response to this incident, the company notified the FBI and all applicable regulatory agencies.

What You Can Do. If you have additional questions, please call our dedicated assistance line at 833-231-3357, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

For More Information. Phishing is a type of electronic attack where outside individuals impersonate a trusted person or company to obtain information, such as email credentials. The company is encouraging potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and to monitor credits reports for suspicious activity and to detect errors. Individuals can obtain a free credit report annually from each of the three major credit reporting bureaus by visiting www.annualcreditreport.com, calling 877-322-8228, or contacting the three major credit bureaus directly at: Equifax, P.O. Box 105069, Atlanta, GA 30348, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; TransUnion, P.O. Box 2000, Chester, PA 19016, 800-680-7289, www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General.

Individuals have the right to place a "security freeze" on their credit reports, which will prohibit a consumer reporting agency from releasing information without their express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in an individual's name without their consent. However, individuals should be aware that using a security freeze to take control over who gets access to the personal and financial information in their

credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, individuals cannot be charged to place or lift a security freeze on their credit reports. Should individuals wish to place a security freeze, they may contact the major consumer reporting agencies listed above. In order to request a security freeze from the consumer reporting agencies, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement or the individual's state Attorney General. This notice has not been delayed by law enforcement. You may have the right to obtain a police report filed in regard to this incident.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. You may also write to ABM at Attn: Legal Department, One Liberty Plaza, 7th Floor, New York, New York 10006.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 134 Rhode Island residents impacted by this incident.

###